CYBER SECURITY FOR BUSINESSES
SDPD Neighborhood Policing Resource Team
August 7, 2012

CONTENTS

Computer crimes involve the illegal use of or the unauthorized entry into a computer system to tamper, interfere, damage, or manipulate the system or information stored in it. Computers can be the subject of the crime, the tool of the crime, or the target of the crime.

As the subject of a crime, a criminal would use your computer or another computer to willfully alter the information stored in your computer, add fraudulent or inaccurate information, delete information, etc. Motives for this include revenge, protest, competitive advantage, and ransom.

As the tool of a crime, a criminal would use a computer to gain access to or alter information stored on another computer. In one common mode of attack a hacker would send a "spear phishing" e-mail to employees who have access to the business bank account. The e-mail would contain an infected file or a link to a malicious website. If an employee opens the attachment or goes to the website, malicious software or malware that gives the hacker access bank account log-ins and passwords would be installed on the computer. The hacker would then have electronic payments made to accounts from which the money would be withdrawn. Criminals also use computers to commit various frauds and steal identities and other information.

As the target of a crime, computers and information stored in them can be stolen, sabotaged, or destroyed. Sabotage includes viruses, malware, and denial-of-service attacks. Trade secrets and sensitive business information stored in computers can be lost in these kinds of attacks.

Your computers and the information in them should be protected as any valuable business asset. The following tips deal with physical and operational protective measures, Wi-Fi hacking and hotspot dangers, personnel policies and employee training, anti-virus and spyware protection, protecting your bank accounts, use of social media, preventing and dealing with data breaches, and safer use of the Internet. For more details see National Institute of Standards and Technology (NIST) Interagency Report NISTIR 7621 entitled *Small Business Information Security: The Fundamentals*, dated October 2009. It's available online under NIST IR Publications on **http://csrc.nist.gov**.

Also, consider joining the FBI's InfraGard, a partnership with the private sector with the goal of promoting an ongoing dialogue and timely communications between its members and the FBI. Its members gain access to information that enables them to protect their assets from cyber crimes and other threats by sharing information and intelligence. Go to **www.infragard.net** to apply for membership.

PHYSICAL PROTECTIVE MEASURES

- Do not allow unauthorized persons to have access to any of your computers. This includes cleaning crews and computer repair persons.
- Install surface or cable locks to prevent computer equipment theft.
- Install computers on shelves that can be rolled into lockable furniture when employees leave their work areas.
- Locate the computer room and data storage library away from outside windows and walls to prevent damage from external events.
- Install strong doors and locks to the computer room to prevent equipment theft and tampering.
- Reinforce interior walls to prevent break-ins. Extend interior walls to the true ceiling.
- Restrict access to computer facilities to authorized personnel. Require personnel to wear distinct, color-coded security badges in the computer center. Allow access through a single entrance. Other doors should be alarmed and used only as emergency exits.

SPECIAL MEASURES FOR LAPTOPS

Special security measures are needed for laptops to prevent them from being stolen and the data in them used to harm your business.

- Train employees in the need for special measures to protect laptops and their data wherever they may be used.
- Issue desktops instead of laptops to employees who seldom leave their offices.
- Have employees lock up their laptops when they are left unattended in their offices. Laptops should never be left unguarded.
- Have employees carry their laptops in a sports bag or briefcase instead of the manufacturer's bag.
- Do not leave a laptop visible inside vehicles or unattended in public places.
- If left unattended, secure the laptop with a cable lock to something that cannot be easily moved. Or install an alarm that will sound if the laptop is moved.
- Create a loss response team to monitor compliance with laptop and data security measures, investigate losses, assess data needs, and remove data no longer needed.

The following measures should be employed to protect your business in the event a laptop is lost or stolen.

- Have employees back up their files so they can be recovered if their laptop is lost or stolen. These back-up files should be kept in a separate, secure place.
- Protect data with strong passwords, i.e., ones that are at least eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol.
- Don't store passwords on laptops.
- Determine if employees need all the data on their laptops to perform their jobs. Remove any data that is not needed.
- Encrypt all sensitive information so it cannot be compromised.
- Install software that will enable you to erase sensitive information when the thief logs onto the Internet.

And the following measures can help you recover a laptop that has been lost or stolen.

- Keep a record of all laptop model and serial numbers so if one is recovered you can prove it is yours. Also keep the sales receipt and register the laptop with the manufacturer.
- Place stickers on the laptops with a phone number to call if one is lost and found by an honest person. But don't put the business name on it. That could be used by criminals to guess passwords or assess the sensitivity of the data stored on the laptop.

- Install hardware, software, or both to aid in recovery of the laptop. After you report the laptop lost or stolen the software enables a monitoring company to track the laptop when the thief logs onto the Internet. Hardware systems work the same but have a Global Positioning System (GPS) device that can pinpoint its location.
- Report the loss to the local law enforcement agency, and notify the manufacturer.
- Look for it on Craigslist and E-Bay.

PROCEDURAL AND OPERATIONAL PROTECTIVE MEASURES

- Classify information into categories based on importance and confidentiality. Use labels such as "Confidential" and "Sensitive." Identify software, programs, and data files that need special access controls. Employee access should be limited to what he or she needs to do their jobs. No employee should have unlimited access, especially to personally identifiable information.
- Reevaluate the access needs of those in senior and supervisory positions as they are promoted within an organization.
- Clearly document and consistently enforce all policies and controls.
- Install software-access control mechanisms. Require a unique, verifiable form of identification, such as a user code, or secret password for each user. Install special access controls, such as a call-back procedure, if you allow access through a dial-telephone line connection.
- Have your Information Technology (IT) manager change administrative password on a regular basis. A number of free tools are available for this if manual modification is not practical. This password should also be changed during non-business hours.
- Require that passwords be a random sequence of more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Passwords should be changed at least every three months and not be shared.
- Employee user accounts should not have administrative privileges. This will prevent the installation of any unauthorized software or malicious code that an employee might activate.
- Change security passwords to block access by employees who change jobs, leave, or are fired. The latter become a high risk to your business for revenge or theft.
- Encrypt confidential data stored in computers or transmitted over communication networks. Use National Institute of Standards and Technology (NIST) data encryption standards.
- Design audit trails into your computer applications. Log all access to computer resources with unique user identification. Separate the duties of systems programmers, application programmers, and computer programmers.
- Review automated audit information and control reports to determine if there have been repeated, unsuccessful attempts to log-on both from within and outside your facility. Look for unauthorized changes to programs and data files periodically.
- Use monitoring or forensic tools to track the behavior of employees suspected of malicious activities. Cyber crimes committed by malicious employees are among the most serious threats to networked systems and data. They can disrupt operations, corrupt data, exfiltrate sensitive information, or compromise an IT system. For more information on insider threats and how to prevent fraud see the *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector* published by the Carnegie Mellon University and Software Engineering Institute, July 2012. It can be downloaded at **www.sei.cmu.edu/reports/12sr004.pdf.**
- Pay closer attention to those in special positions of trust and authority, e.g. accountants and managers, because it is easier for them to commit high-value crimes.
- Monitor incoming Internet traffic for signs of security breaches.
- Make backup copies of important business information, i.e., documents, spreadsheets, databases, files, etc. from each computer used in your business. This is necessary because computers die, hard disks fail, employees make mistakes, malicious programs can destroy data, etc. Make backups automatically at least once a week if possible. Test the backups periodically to ensure that they can be read reliably. Make a full backup once a month and store it in a protected place away from your business.
- Delete all information stored in your printers, copiers, and fax machines at least once a week. Use a secure data deletion program that will electronically wipe your hard drives. Simply hitting the delete key will leave some data on the hard drive.

- Be careful in getting outside help with computer security problems. Call the San Diego District Office of the U.S. Small Business Administration at **(619) 727-4883** for advice and recommendations. Start with a list of vendors or consultants. Then define the problem, send out a request for quotes, examine each quote, and check the provider's references and history before hiring one.
- If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Crime Center NW3C, at **www.ic3.gov**. The IC3 website also includes tips to assist you avoiding a variety of Internet frauds.
- Develop a response plan to control the damage that can result from malicious insider activity. The response team would assist in investigating the fraud and use the lessons learned to prevent further fraud and improve the plan.

PERSONNEL POLICIES AND EMPLOYEE TRAINING

Employees can do a great deal of damage to a business by ignorance of security policies, negligence in protecting business secrets, deliberate acts of sabotage, and the public release of sensitive information. The following measures will help prevent this. Before implementing them be sure to consult with legal counsel to ensure compliance with federal, state, and local laws.

- Conduct a comprehensive background check on prospective employees. Check references, credit reports, criminal records, and schools attended.
- In considering criminal record information in making employment decisions, follow the U.S. Equal Employment Opportunity Commission (EEOC) Enforcement Guidance No. 915.002 dated 4/25/2012 regarding the prohibition of discrimination under Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e *et seq*. Best practices for employers include the following:
  - Eliminate policies or practices that exclude people from employment based on any criminal record.
  - Train managers and hiring officials in the EEOC Enforcement Guidance.
  - Develop a policy and narrowly-tailored procedures for screening applicants and employees for criminal conduct.
  - Identify essential job requirements and the actual circumstances under which the jobs are performed.
  - Determine the specific offenses that may demonstrate unfitness for performing such jobs.
  - Identify the criminal offenses based on all available evidence.
  - Determine the duration of exclusions for criminal conduct based on all available evidence.
  - Include procedures for individualized assessments.
- Interview prospective employees. Seek to hire individual who are team-oriented, can respond well to criticism, and can deal well with conflicts, i.e., ones unlikely to become insider threats.
- Require vendors, suppliers, and other contractors to use similar standards in hiring their employees. Include language in all contracts that makes contractors liable for actions of their employees.
- Treat all employees fairly and make sure none are teased by their peers or supervisors because of their ethnicity, speech, financial situation, social skills, or other traits.
- Monitor activities of employees who handle sensitive or confidential data. Watch for employees who work abnormally long hours, weekends, or holidays, or who refuse to take time off. Many computer crime schemes require regular, periodic manipulation to avoid detection. Also watch for employees who collect material not necessary to their jobs, such as data printouts, software manuals, etc.
- Conduct periodic background checks on existing employees and look for unexplained financial gains
- Train your employees in your basic computer usage and security policies. Also cover penalties for not following your policies. And have employees sign a statement that they understand and will follow your policies.
- Train your employees about security concerns and procedures for handling e-mails, clicking on links to websites, responding to popup windows, and installing USB drives. For example, they should not open e-mail from an unknown sender, open unexpected e-mail attachments, click on any links in e-mail messages even if they look real, respond to popup windows, or install personal USB drives. As for USB drives, you should supply your employees with ones that have built-in encryption.
- Train your employees to be aware of what others, even their supervisors, are doing and to report any suspicious behavior that threatens your security.
- Conduct periodic re-training because people forget things. Use pamphlets, posters, newsletters, videos, etc.

- Prohibit your employees from using their work computers for online shopping. There is a chance that they might unwittingly land on a fake website with an address similar to that of a legitimate company, e.g., Appple.com instead of Apple.com. This would inadvertently expose your computer network to cyber attacks.
- Spread security training over time. Don't rely on one-time seminars by security professionals. Present information in small pieces.
- Make security messages visible. Use videos in training sessions. Put up posters at fax machines, shred bins, coffee rooms, and other places where employees gather. Change them at least once a month. Have a security column in the company newsletter.

MALWARE PROTECTION

The following measures can help protect your computer from viruses, spyware, and other types of malware:

- Keep your computer up to date with the latest hardware and software firewalls and anti-virus, anti-spyware, and anti-adware software. The latter are designed to protect against software that either self-installs without your knowledge or is installed by you to enable information to be gathered covertly about your Internet use, passwords, etc. This kind of software is often installed when you visit websites from links in e-mails. This also applies to multi-function printers, fax machines, and copiers that can be accessed using a web browser.
- Also install real-time e-mail and web security along with solutions that prevent data theft and loss of confidential information. Traditional anti-virus and spyware products don't provide this protection.
- Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information.
- Do not buy or download free anti-spyware software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected malicious software.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the ad. To be safe on a PC, hold down the Ctrl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full anti-virus scan.
- Do not respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 8, which is designed to prevent phishing attacks. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Do not install files or programs from CDs or flash drives before checking them for viruses.
- Scan demo disks from vendors, shareware, or freeware sources for viruses.
- Restrict use of electronic bulletin boards.
- Do not download files from unknown sources.
- Do not allow any website to install software on your computers.
- Scan downloaded files for viruses. Avoid downloading executable files.
- Obtain copies of your anti-virus software for your employees' home computers your employees do some business work at home. Also ensure that your employees' home computers are protected by hardware and software firewalls between their system(s) and the Internet.

PROTECTING BANK ACCOUNTS

- Set up dual controls so that each transaction requires the approval of two people.
- Establish a daily limit on how much money can be transferred out of your account.
- Require all transfers be prescheduled by phone or confirmed by a phone call or text message.

- Require that all new payees be verified.
- Check bank balances and scheduled payments at the end of every workday, rather than at the beginning, and contact the bank immediately if anything is amiss. Timely action can halt the completion of a fraudulent transaction because transfers usually aren't made until the next morning.
- Inquire about your bank's defenses against cyberattacks and review the terms of your banking agreement with regard to responsibilities for fraud losses. Shop around for banks that provide better protections.
- Conduct online business only with a secure browser connection, which is usually indicated by a small lock in the lower right corner of your web browser window. Erase your browser cache, temporary Internet files, cookies, and history after all online sessions. This will prevent this information from being stolen if your system is compromised.

USE OF SOCIAL MEDIA

While the use of social media can stimulate innovation, create brand recognition, generate revenue, and improve customer satisfaction, it has inherent risks that can negatively impact business security. Thus businesses need to develop a social media strategy and a plan to address the risks of business and employee use. These risks include the following:

- Data leakage or theft
- Data system downtime to clean viruses and malware
- Exposure of customer confidential information
- Spear phishing attacks on customers and employees
- Adverse legal actions
- Privacy violations
- Brand and reputation damage
- Loss of competitive advantage
- Infection of mobile devices
- Productivity loss from excessive employee use
- Circumvention of business controls

Some risk mitigation techniques for business and employee use of social media are listed below. For details on risks and mitigation techniques see the emerging technology white paper entitled *Social Media: Business Benefits and Security, Governance and Assurance Perspectives* published by the Information Systems Audit and Control Association (ISACA).

- Conduct awareness training to inform employees of the risks in using social media.
- Ensure that anti-virus and anti-malware controls are updated daily.
- Use content filtering to restrict or limit access to social media sites.
- Provide employees with clear guidelines regarding what information about the business can and cannot be posted on their personal sites.
- Limit use of social media on business computers and devices.
- Scan the Internet for unauthorized or fraudulent use of the business name or brand, or hire a brand-protection firm to do this.
- Require strong passwords for site access by its managers.
- Give customers periodic information updates to maintain awareness of potential fraud.
- Establish policies for the use of mobile devices to access social media.
- Install appropriate controls on mobile devices.
- Obtain access to employees' personal sites and monitor them for security breaches.

PREVENTING AND DEALING WITH DATA BREACHES

The five key principles defined by the Federal Trade Commission in a paper entitled *Protecting Personal Information: A Guide for Business* at **http://business.ftc.gov/privacy-and-security/data-security** will help you

protect personal information in your business and prevent data breaches. They are: (1) Take stock, (2) Scale down, (3) Lock it, (4) Pitch it, and (5) Plan ahead. You should do the following for each.

1. Take stock: Know what personal information you have in your files and in your computers.

- Inventory all file-storage and electronic equipment. Know where your business stores sensitive data.
- Talk to your employees and outside service providers to determine who sends you personal information and how it is sent.
- Consider all the personal information you collect from customers, and how you collect it.
- Review where you keep the information you collect, and who has access to it.

2. Scale down: Keep only what you need for your business.

- Use Social Security Numbers (SSNs) only for required and lawful purposes. Don't use them for employee or customer identification.
- Keep customer credit or debit card information only if you have a business need for it. Don't keep any information you don't need.
- Change the default settings on your software that reads customer's credit or debit cards.
- Review the credit application forms and fill-in-the-blank web screens you use to collect data from potential customers, and eliminate requests for any you don't need.
- Use no more that the last five digits of credit or debit card numbers on electronically printed receipts that you give to your customers. And don't use the card's expiration date.
- Develop a policy for retaining written records that is consistent with your business needs and the law.

3. Lock it: Protect the information that you keep and transmit.

- Keep documents and other materials containing personal information in locked rooms or file cabinets.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Create a security policy for your employees when using laptops in and out of your office. (See prior section on Special Measures for Laptops.)
- Control access to your building.
- Encrypt sensitive information you send over public networks or use a secure file transfer service. Don't send personal information by e-mail.
- Run up-to-date anti-virus and anti-spyware programs on all your computers. Use a firewall to protect your computers and network. (See prior section on Anti-virus and Spyware Protection.)
- Require employees to use strong passwords.
- Set access controls so employees only have access to information they need for their jobs. (See prior section on Procedural and Operational Protective Measures.)

4. Pitch it: Properly dispose of what you no longer need.

- Create and implement secure information disposal practices for employees in your office and for those who travel or work at home.
- Train your staff to separate sensitive and other paper records. Dispose of the former by shredding, burning, or pulverizing them. Use cross-cut shredders. The latter can be put in the trash.
- Make shredders available throughout your office, especially next to the copiers.
- Remove and destroy the hard disk of any computer or copier headed for the junkyard. Or wipe them securely.
- Remove and securely wipe hard drives of rented copiers before returning them. Or clear the memory and change the pass codes.
- Destroy CDs, floppies, USB drives, and other data storage devices, or securely wipe them before disposal.
- Test how thoroughly factory resets and remote wipes destroy data on any smartphones your employees use in the business, and only permit them to use phones on which the data can be completely destroyed when the device is

retired. If there is any doubt about this, use a hammer on the phone to make sure it does not get into the secondary market.

5. Plan ahead: Create a plan for dealing with security breaches.

- Organize a response team and designate a team leader to manage the activities.
- Draft contingency plans for dealing with various kinds of breaches, including hacking, lost laptop, etc.
- Investigate breaches immediately and take steps to eliminate existing vulnerabilities or threats to personal information.
- Disconnect a compromised computer from the Internet.
- Post information about the breach on your website and include the phone number and e-mail address of your customer service staff.
- Create a list of who to notify inside and outside of your business in the event of a breach. The latter include the appropriate law enforcement agencies, the persons whose information has been compromised, your customers and other businesses that may be affected, and the media.
- Draft notification letters and other written communications. Consult your attorney for state and federal notification requirements.
- Consider what outside assistance is needed, e.g., in forensics, media relations, etc.

Note that California Civil Code Sec. 1798.82 requires businesses to notify persons whose personal information has been compromised and specify the information involved. The notice requirement is triggered if the breach involves a person's name in combination with any of the following: Social Security Number; driver's license or California Identification Card number; financial account, credit card, or debit card number along with any PIN or other access code required to access the account; medical information; or health insurance information. The letter of notice should also recommend measures to take to deal with the breach, warn of attempts to obtain personal information by e-mail, and ask that any such attempts be reported to your customer service staff immediately.

SECURITY PLANNING

One way small businesses can improve their cyber security is to use the Small Biz Cyber Planner that was created by the Federal Communications Commission (FCC) in collaboration with public and private sector partners, including the Department of Homeland Security, the National Cyber Security Alliance, and the Chamber of Commerce. It can be created and generated at **www.fcc.gov/cyberplanner**.

This planning guide is designed for businesses that lack the resources to hire a dedicated staff to protect themselves and their customers from cyber threats. Even a business with one computer or one credit card terminal can benefit from this tool. However, the FCC recommends that businesses using more sophisticated networks with dozens of computers also consult a cyber security expert on using the cyber planner. And the FCC provides no warranties with respect to the guidance provided by this tool and is not responsible for any harm that might occur from using it. The planner deals with the following topics.

- Privacy and Data Security. Nothing is more important than the security of your data. How you handle and protect it is central to the security of your business and the privacy expectations of all the people involved.
- Scams and Fraud. Telecommunication technology offers cyber criminals many ways to victimize your business, scam your customers, and hurt your reputation. You need to be aware of the most common online scams.
- Network Security. For this you need to: (1) identify all devices and connections on the network, (2) set boundaries between your systems and others, and (3) enforce controls to ensure that unauthorized access, misuse, or denial-of-service attacks can be thwarted or rapidly contained, and that your systems can recover from these threats.
- Website Security. Web servers that host the data and other content available to the public on the Internet are the most targeted components of a business' network. Cyber criminals are constantly looking for websites to attack. Thus it is essential that your servers and the network infrastructure that supports them be secure because a breach can cause loss of revenues and customer trust, and legal liability.
- E-mail. E-mail has become vital for everyday operations. It must be secure to ensure the privacy of its users and to protect customer and business information.

- Mobile Devices. Mobile devices such as smart phones, tablets and Wi-Fi enabled laptops, if not secure, can expose and compromise all your business networks.
- Employees. Businesses must establish formal recruitment and employment processes to control and preserve the quality of their employees. Otherwise they risk workplace violence, theft, embezzlement, lawsuits for discrimination in hiring, and other workplace problems.
- Facility Security. Protecting those who work in and visit your business should be one of your top priorities.
- Operational Security. These measures are designed to deny hackers access to any information about your operations and plans.
- Payment Cards. These measures prevent fraud, keep customer information safe, and enable you to meet obligations to your bank or payment services processor.
- Incident Response and Reporting. Even well-implemented security measures cannot prevent all breaches, so be sure to have procedures in place to respond to breaches if they occur.
- Policy Development and Management. All businesses should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputation, and discouraging inappropriate behavior by employees. These need to be tailored to your business and updated when needed to deal with new threats and problems.

WI-FI HACKING AND HOTSPOT DANGERS

Use of Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places pose major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure. If it asks for a password through your browser simply to grant access, or it asks for a Wired Equivalent Privacy (WEP) password, it's best to treat it as unsecured. You can be more confident that a hotspot is secure only if it asks for the Wi-Fi Protected Access (WPA and WPA2) password. WPA2 is more secure. However, a flaw in a feature added to Wi-Fi called Wi-Fi Protected Setup (WPS) allows WPA and WPA2 security to be bypassed and broken by brute force in many situations.

Also, unsecure laptops and smart phones make it easy for a hacker to intercept information to and from the web, including passwords and credit or debit card numbers. They are also vulnerable to virus and spyware infections, and to having their contents stolen or destroyed. A hacked laptop or smart phone can also create a security risk for the user's workplace if it contains a password to the corporate network. Wi-Fi users should take the following steps to reduce these risks:

- Turn the Wi-Fi on your laptop, PDA, and smart phone off when you aren't using the network. Otherwise your Wi-Fi card will broadcast your Service Set Identifier (SSID) looking for all networks it was previously connected to. This enables hackers to figure out the key that unscrambles the network password.
- Use a known service instead of Free Public Wi-Fi or similar risky, unknown signals called ad hoc networks.
- Check the Wi-Fi security policies of your service provider and install the protections they offer to ensure it's a known network and not an "evil twin" hacker site pretending to be the legitimate one.
- Pay attention to warnings that a Secure Sockets Layer (SSL) certificate is not valid. Never accept an invalid certificate on a public wireless network. Log off and look for a trustworthy network. Look for the padlock indicating an SSL connection. Keep your firewall on. And keep your operating system updated.
- Find out if your company offers a Virtual Private Network (VPN) and learn how to use it. Encrypted VPN sessions offer the highest security for public wireless use. Use Hypertext Transfer Protocol Secure (HTTPS) when accessing a website or use a VPN to protect the transmission of sensitive information when using a wireless connection.
- Upgrade your Wi-Fi cards. The older WEP security is easily hacked. The new WPA and WPA2 are much more resistant to attack.
- Secure IEEE 802.11 wireless access points with a WPA2 and Advanced Encryption Standard (AES) encryption to protect sensitive communications.
- If your router has the WPS function, disable it. Methods have been published for doing this for some models. But on others, disabling the WPS in the user interface is not effective and the device remains vulnerable to attack.

- Learn to connect securely. Even the vulnerable WEP offers more privacy and protection than an unsecured public connection. It's not something the average hacker can crack. Make sure your connection is legitimate. Look at your connection page for a name and description. A legitimate wireless network is simply called a "wireless network." It will display an icon of just one connected computer. So called ad hoc or peer-to-peer networks that are used by scammers to steal your personal information scammers are not legitimate. The will be called "computer-to-computer" networks and display an icon of several computers connected together. Never connect to this network. And be sure to set up your computer so it doesn't automatically connect to a network but allows you to choose a connection.
- Only log in or send personal information on website pages that are encrypted. They will have **https://** or **shttp://** in their addresses and a "lock icon" at the top or bottom of your browser window. You can click on this icon to display information about the website and help you verify that it's not fraudulent.
- Use a different password for each account.
- When you've finished using an account, log out. Don't stay signed in.
- Pay attention to warnings from your browser if you try to visit a fraudulent website or download a malicious program.
- Remove all passwords and browsing history after using a shared computer.
- Disable file-sharing on your laptop.
- Don't send any sensitive personal or business information while in a hotspot unless you absolutely have to.
- Put strong passwords on your wireless network. Passwords should be more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Other advice on creating strong passwords can be found at **www.microsoft.com/protect/yourself/password/checker.mspx.**
- Be aware of the existence of malware that enables a mobile phone to be used as an open microphone with or without the owner's knowledge.

Your IT manager should also do the following to protect corporate data from hotspot dangers:

- Establish and enforce strong authentication policies for devices trying to access corporate networks.
- Require employees to use a corporate VPN and encryption when making connections and exchanging data. Better still, set up computers so that devices automatically connect to the VPN and encrypt data after making sure that the computer or device hasn't been lost or stolen.
- Make sure all devices and software applications are configured properly and have the latest patches.
- Ensure that corporate security policies prevent employees from transferring sensitive data to mobile devices or unauthorized computers.
- Provide employees with broadcast air cards that require a service plan so they don't have to use public hotspots for wireless connections.

SAFER USE OF THE INTERNET

There are presently two similar efforts by the U.S. Government to promote safer use of the Internet. The one by the FTC's Bureau of Consumer Protection is called Stop.Think.Click. The other, developed by a group representing industry, government, academia, and the nonprofit sector in 2009, and promoted by the Obama administration and the Department of Homeland Security, is called Stop.Think.Connect.

Stop.Think.Click

This effort defines seven practices for safer computing and provides tips on preventing identity theft, safe use of social networking sites, online shopping, Internet auctions, avoiding scams, and wireless security. It also provides a glossary of terms. The seven practices are:

1. Protecting your personal information
2. Knowing who you're dealing with
3. Using anti-virus and anti-spyware software, as well as a firewall
4. Setting up your operating system and web browser software properly, and updating them regularly
5. Protecting your passwords

6. Backing up your important files
7. Learning who to contact if something goes wrong online.

Go to **www.ftc.gov/bcp/edu/pubs/consumer/tech/tec15.pdf** for information about these practices and tips.

Stop.Think.Connect

This effort suggests that users do the following:

- Stop. Before you use the Internet take time to understand the risks and learn how to spot potential problems
- Think. Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact the safety of yourself and your family.
- Connect. Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

You can learn how to become a partner in this effort by going to its website at **www.stopthinkconnect.org**. This site also contains the tips and advice for doing the following.

Keeping a clean machine:

- Have the latest security software, web browser, and operating system.
- Use programs that automatically connect and update your security software.
- Protect all devices that connect to the Internet from viruses and malware.
- Use your security software to scan all USBs and other external devices before attaching them to your computer.

Protecting your personal information:

- Secure your accounts with protection beyond passwords that can verify your identity before you conduct business.
- Use passwords that are more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol.
- Use different passwords for every account.
- Keep a list of your passwords stored in a safe place away from your computer.
- Use privacy and security settings to limit who you share information with.

Connecting with care:

- Delete any suspicious e-mail, tweets, posts, and online advertising.
- Limit the business you conduct from Wi-Fi hotspots and adjust your security settings to limit who can access your computer.
- Use only secure websites when banking and shopping, i.e., ones with **https://** or **shttp://** in their addresses.

Being web wise:

- Keep pace with new ways to stay safe online by checking trusted website for the latest information.
- Think before you act when you are implored to act immediately, offered something that sounds too good to be true, or asked for personal information.
- Back up your valuable information by making an electronic copy and storing it in a safe place.

Being a good online citizen:

- Practice good online safety habits.
- Post about others as you would have them post about you.
- Report all types of cybercrime to you local law enforcement agency and other appropriate authorities.